	201901100 - Shubham Patel
	Paga No. : 1
	50401 - Homework 4 Date:
[1]	Here, 248 mod 97=1
	Here, 248 mod 97=1
	4 48 2000 97 = 1
	$\frac{4^{48} \mod 97 = 1}{5^{48} \mod 97 = 96}$ and 5 mod 97 = 35
	32 200 77 - 76
	and 5 mod 97 = 35
	B. H.
	30, the smallest premitive element
. 50 -	modulo 97 mis 15. 8222 201
	1 000 6 mm (817 hamp 12 = 6368 2001
[2]	(ham) CPP
ري	For, m=pq ip and q are distinct odd primes
. (3	1 Samaric ash manage 132 Trains you
	7(m)= (p-1) (q-1)=0PE = E228 = pni
	ged (p-1, 9-1)
	$(p^2)\times (p)\times (p)\times (p)\times (p)\times (p)\times (p)\times (p)\times (p$
. Cai 4	and ug-je q'd'ham a miller de l'and ug-1=p'd
(1 house)	candiciate d'allance e = 113 21 a. por
	Them, \(\ample \tem) = p \q' \d(= \cop1) \q' = p \cq-1)
	we have, ab = 1 (mod 7(n)),
18	- a consolite (2 cm) (+1) = K(p-1)q'+1
	Then, colfi, alash pol
	$\alpha^{ab} \equiv \alpha^{k(p-1)q+1} \pmod{p} \equiv \alpha \pmod{p}$
	Similarly, of ap = xk(q-1)pi+ cmod q) = x (mod q)
	since, ocab = occomod p) mod ocab = mod q.
	Then, $x^{ab} \equiv x^{k(p-1)}q^{l+1} \pmod{p} \equiv x \pmod{p}$ Similarly, $x^{ab} \equiv x^{k(q-1)p^{l+1}} \pmod{q} \equiv x \pmod{q}$ Since, $x^{ab} \equiv occmod p$) mod $x^{ab} \equiv \mod{q}$. It follows their $x^{ab} \equiv x \pmod{q}$.

	in the company of the contract
	2 mgo No.: 2
	A decomposition of the control of th
	(1) 1-C 200 200 and Acon 2-2808
	(b) d=6, λ(m)= 468 and φ(m)=2808 b'mod λ(m)=67 and b'mod Φ(m)=2407
	b mod A(n) = 67 and 0 11/00 (har)=
[3]	28702 = (2)×(1/3) ×(127)
	$28702 = (2) \times (113) \times (127)$
	wo Andi their to it
	100 0503 = 1.6mod 2)
	1095 8563 = 1 (mod 2); 1095 8563 = 1095 8563 = 1095 8563 = 1095 8563 = 1095
	1095 5563 = 61(1000 C) 39 (mod 127)
	sin and plants in the second second second
2-years	By chimese reminder theorem,
	logs 8563 = 3903 :01 (1)
	C-6-1-07 /030
->	31152 = (9)4 x (3) x(11) x (59)
4	are find that 109,012611=14 (mod 16).
	109,012611 = 2 mod (3), 109,01261) = 8 (mod 16),
1.	and logio 12611= 51 cmod 59)
	Lifema bases is in and as
14.7.1	By chimese reminder theorem,
	10910 12611 = 17102.
ra karek	
	-a harman in a single of the second of the s
	Ada Lanco Carlos and a secondary of the

	Page No. 1
	Data:
[4]	a) Points on the elliptic curve
	$y^2 = x^3 + x + 28$ define over 771
	We make table of oc. oc3+oc+28 mod ?=
	quadratic residue and y points
	We get 72 number of points by
	doing that.
100 100 20	Car Allord Cancel has some and a
	(b) If & were eyclic; there would
	be points howing order 72 but
	there are no such points.
7	(c) The maximum order of point
	js 36. : /
	(4,5)/is a point having order 36. [Eis isomorphic to Z36 x Z2]
	[Eis isomorphic to Z36 x Z2]
<u> </u>	Minney Francisco Parti Alles
[5]	First,
47 - 1/1	K= (x,-xe)(s,-8,) mod (p+)
	= -22425 x 10915 mod 31846
	=1165

)	7-70 No.; 4
1	Cafe:
	To determine a. we will solve
	companence:
	ra = oc1 - K8, (mod p-1)
	review of the other and
	For lot this comprisence
	simplifies to.
4.3	-93972 a = 23704 (mod 31846)
	1, 16 6 10 6
	we have, ged (23972, 31846)=2 and
	2123704, 30 congruence is
	equivalent to produce of
	11986, a = 11852 (mod 15923)
	This congruence has solution,
	a= 11852 × 11986 (mod 15923)
	= 7459.(mod:15923)
	So, a = 7459 or a = 7459+ (p-1)(2)
	= 23382
Western	
-	By compating x 7459 mod p=125703=B
	and 23382 mod p= 6144 + B
77 - 18 - 18 - 18 - 18 - 18 - 18 - 18 -	we see theet,
	C = 7459

	Date:
[6]	@ Signature (20679, 11082) on the
	messeige m = 20543.
	5 20543 mod 31847 = 20688
	$\frac{messege}{5^{20543}mod31847} = 20688$ $= 26379 20679 mod31847$
	(6) By solving instance of discrete
	logarithm, a= logs 26379 = 7973
***************************************	(c) To determine 'k', we solve the
	coudane vice
	$kS \equiv \alpha - \alpha r \pmod{p-1}$
_	for, K. This conquence simplifies to,
	for, K. This congruence simplifies to,
	gcd (11082, 31846)=2
	and 2/13618, so congruence is equivalent to 5541 k = 6809 (mod 15923)
	this congruence has the solution,
	K = 6,809 x 5541-1 cmod 15923 = 3464 (mod 15923)
_	Therefore, k= 3464 mor k=7459+(p-D12=
	[2] 사용장에 가입되는 이 처른 전에서 하나 있다. 나가는 아마리를 하고 있다면 하나 있는 사람이 이 없는 그 물론은 학생 경험을 잃었다면 사용하다면 했다.
	By computing a mod p=11168+x
	By computing a 3464 mod p=11168 = x and a 19387 mod p=20679=x,
	we see theet, K=19387.
The state of the s	나는 아들은